



DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITE DE COOPERATION EN MATIÈRE DE BREVETS (PCT)

(51) Classification internationale des brevets ⁶ : G06K 19/073	A1	(11) Numéro de publication internationale: WO 99/49416 (43) Date de publication internationale: 30 septembre 1999 (30.09.99)
(21) Numéro de la demande internationale: PCT/FR99/00583 (22) Date de dépôt international: 16 mars 1999 (16.03.99) (30) Données relatives à la priorité: 98/03471 20 mars 1998 (20.03.98) FR (71) Déposant (pour tous les Etats désignés sauf US): GEMPLUS S.C.A. [FR FR], avenue du Pic de Bertagne, Parc d'Activités de Gémenos, Boite postale 100, F-13881 Gémenos Cedex (FR). (72) Inventeurs; et (75) Inventeurs/Déposants (US seulement): FEYT, Nathalie [FR/FR]; Bâtiment 6, 20, rue du Lieutenant J.P. Meschi, F-13005 Marseille (FR). BENOIT, Olivier [FR/FR]; 22, rue Rastegue, F-13400 Aubagne (FR). NACCACHE, David [FR/FR]; 7, rue Chaptal, F-75009 Paris (FR). (74) Mandataire: NONNENMACHER, Bernard; Gemplus S.C.A., avenue du Pic de Bertagne, Parc d'Activités de Gémenos, F-13881 Gémenos Cedex (FR).		(81) Etats désignés: CA, CN, IN, JP, SG, US, brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE). Publiée <i>Avec rapport de recherche internationale.</i>

(54) Title: DEVICES FOR HIDING OPERATIONS PERFORMED IN A MICROPROCESSOR CARD

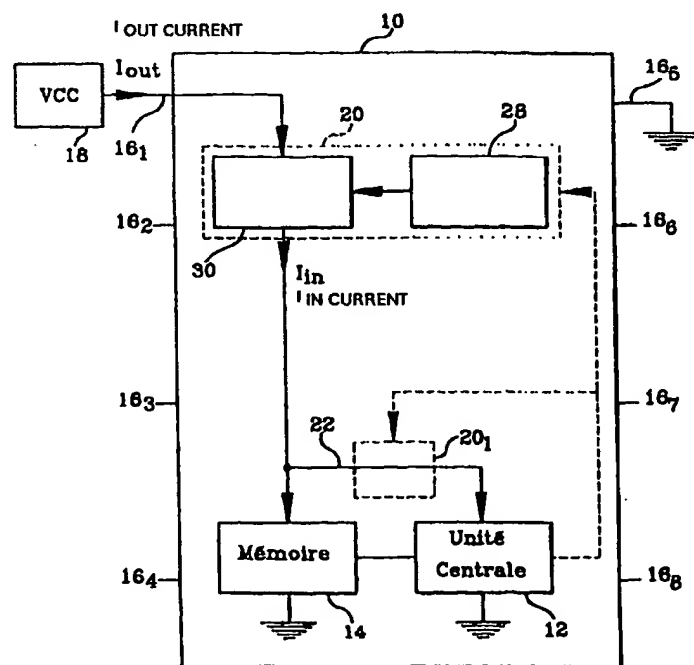
(54) Titre: DISPOSITIFS POUR MASQUER LES OPERATIONS EFFECTUEES DANS UNE CARTE A MICROPROCESSEUR

(57) Abstract

The invention concerns microprocessor cards and, in such cards, various devices for hiding operations performed in the card against fraudulent breaches by analysing the current consumed. The invention is characterised in that it consists in adding in the card a device (20) modifying the consumed current, either by averaging it by integration, or by adding thereto random values by a random signal generator (28) so as to hide the operations performed. In another embodiment, it consists in carrying out simultaneously an operation for making secure and writing in an EEPROM memory, the latter generating chaotic current variations which hide the operation to be made secure.

(57) Abrégé

L'invention concerne les cartes à microprocesseur et, dans de telles cartes, différents dispositifs pour masquer les opérations effectuées dans la carte contre les intrusions frauduleuses par l'analyse du courant consommé. L'invention réside dans le fait d'ajouter dans la carte un dispositif (20) qui modifie le courant consommé, soit en le moyennant par une intégration, soit en lui ajoutant des valeurs aléatoires par un générateur de signaux aléatoires (28) de manière à masquer les opérations effectuées. Dans une variante, il est prévu d'effectuer simultanément une opération à sécuriser et l'écriture dans une mémoire EEPROM, cette dernière créant des variations de courant chaotiques qui masquent l'opération à sécuriser.



18...POWER CIRCUIT
14...MEMORY
12...CENTRAL PROCESSING UNIT

UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie	ES	Espagne	LS	Lesotho	SI	Slovénie
AM	Arménie	FI	Finlande	LT	Lituanie	SK	Slovaquie
AT	Autriche	FR	France	LU	Luxembourg	SN	Sénégal
AU	Australie	GA	Gabon	LV	Lettonie	SZ	Swaziland
AZ	Azerbaïdjan	GB	Royaume-Uni	MC	Monaco	TD	Tchad
BA	Bosnie-Herzégovine	GE	Géorgie	MD	République de Moldova	TG	Togo
BB	Barbade	GH	Ghana	MG	Madagascar	TJ	Tadjikistan
BE	Belgique	GN	Guinée	MK	Ex-République yougoslave de Macédoine	TM	Turkménistan
BF	Burkina Faso	GR	Grèce	ML	Mali	TR	Turquie
BG	Bulgarie	HU	Hongrie	MN	Mongolie	TT	Trinité-et-Tobago
BJ	Bénin	IE	Irlande	MR	Mauritanie	UA	Ukraine
BR	Brésil	IL	Israël	MW	Malawi	UG	Ouganda
BY	Bélarus	IS	Islande	MX	Mexique	US	Etats-Unis d'Amérique
CA	Canada	IT	Italie	NE	Niger	UZ	Ouzbékistan
CF	République centrafricaine	JP	Japon	NL	Pays-Bas	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norvège	YU	Yougoslavie
CH	Suisse	KG	Kirghizistan	NZ	Nouvelle-Zélande	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	République populaire démocratique de Corée	PL	Pologne		
CM	Cameroun	KR	République de Corée	PT	Portugal		
CN	Chine	KZ	Kazakhstan	RO	Roumanie		
CU	Cuba	LC	Sainte-Lucie	RU	Fédération de Russie		
CZ	République tchèque	LI	Liechtenstein	SD	Soudan		
DE	Allemagne	LK	Sri Lanka	SE	Suède		
DK	Danemark	LR	Libéria	SG	Singapour		
EE	Estonie						

DISPOSITIFS POUR MASQUER LES OPERATIONS EFFECTUEES DANS
UNE CARTE A MICROPROCESSEUR

L'invention concerne les cartes à microprocesseur et, dans de telles cartes, différents dispositifs pour masquer les opérations effectuées dans la carte dans le but d'améliorer la sécurité contre les intrusions frauduleuses.

Les cartes à puces se divisent en plusieurs catégories, à savoir :

- les cartes à simple mémoire,
- les cartes à mémoire dite carte intelligente, et
- les cartes à microprocesseur.

Une carte à simple mémoire permet d'effectuer des opérations de lecture et d'écriture dans la zone de mémoire morte électriquement effaçable de façon libre. Une telle carte est d'un faible coût mais elle ne présente pas une sécurité suffisante de sorte qu'elle est de moins en moins utilisée.

Une carte à mémoire intelligente améliore notamment la sécurité des opérations de lecture/écriture en les autorisant seulement lorsque certaines conditions réalisées sous forme câblée sont remplies.

Une carte de la troisième catégorie contient un microprocesseur capable d'exécuter des programmes enregistrés dans une mémoire et d'effectuer ainsi des calculs avec des données secrètes inaccessibles au monde extérieur à la carte. Ainsi, une clé enregistrée dans la mémoire peut servir à valider une transaction électronique telle qu'un achat ou une ouverture de porte sans avoir à être manipulée à l'extérieur de la carte.

Malheureusement, certains microprocesseurs présentent des consommations de courant qui dépendent des calculs effectués à l'intérieur de la carte. Ainsi, un calcul cryptographique comprenant une arborescence
5 de calcul qui dépend des chiffres de la clé utilisée aura différentes empreintes de consommation de courant selon la valeur de la clé utilisée. Il en résulte qu'un fraudeur pourrait corrélér l'empreinte de consommation de courant de la clé utilisée et ainsi remonter à la
10 valeur de la clé.

Pour empêcher cette corrélation, une contre-mesure courante consiste à programmer l'algorithme cryptographique d'une manière telle que quelle que soit la valeur de la clé, l'algorithme passera toujours les
15 mêmes étapes de calcul.

De nombreux algorithmes dits "orientés octets" se prêtent bien à ce mode de programme mais d'autres posent quelques problèmes techniques qui ne sont surmontables qu'au prix de performances calculatoires
20 moins optimales.

La présente invention a donc pour but de mettre en oeuvre dans les cartes à microprocesseur des dispositifs pour masquer les opérations effectuées tout en permettant au programmeur le libre-choix des règles
25 de programmation, qu'elles soient du type "orientées octets" ou non.

Ce but est atteint en modifiant ou brouillant la consommation de la carte de manière que son empreinte soit indépendante des calculs effectués.

30 Cette modification ou ce brouillage de l'empreinte peut être obtenue en ajoutant dans la carte un dispositif qui modifie la consommation de courant.

Dans un premier exemple de réalisation, ce dispositif consomme de la puissance électrique de

manière irrégulière ou aléatoire qui s'ajoute à celle de la consommation normale.

Dans un deuxième exemple de réalisation, ce dispositif réalise une consommation moyenne en
5 réalisant, par exemple, une intégration du courant consommé.

Dans un troisième exemple de réalisation, ce dispositif déclenche le circuit de programmation ou d'effacement de la mémoire du microprocesseur qui
10 consomme de la puissance de manière chaotique, puissance qui masque la consommation due aux opérations effectuées par le microprocesseur pendant la programmation ou l'effacement de la mémoire.

D'autres caractéristiques et avantages de la
15 présente invention effectueront à la lecture de la description suivante d'exemples particuliers de réalisation, ladite description étant faite en relation avec les dessins joints dans lesquels :

- la figure 1 est un schéma fonctionnel d'un
20 premier exemple de réalisation de l'invention,
- la figure 2 est un schéma fonctionnel d'un deuxième exemple de réalisation de l'invention, et
- la figure 3 est un schéma fonctionnel d'un troisième exemple de réalisation de l'invention.

25 Sur les figures qui montrent chacune schématiquement différents moyens pour réaliser l'invention, la puce électronique 10 contenant le microprocesseur de la carte comprend une unité centrale 12 et au moins une mémoire 14, par exemple du type
30 connu sous l'acronyme anglo-saxon EEPROM FOR ELECTRICALLY ERASABLE PROGRAMMABLE READ ONLY MEMORY. Cette puce électronique présente plusieurs bornes d'entrée et/ou de sortie 16_1 à 16_8 dont l'une d'entre elles référencée 16_1 est connectée à un circuit

d'alimentation électrique 18 de tension V_{CC} tandis que celle référencée 16₅ est connectée à la masse.

Le circuit d'alimentation 18 alimente les différents éléments de la puce électronique 10 avec un
5 courant I_{out} et, notamment, la mémoire 14 et l'unité centrale 12. Ce courant I_{out} varie en fonction des opérations effectuées par l'unité centrale et la mémoire et reflètent donc les calculs cryptographiques, ce qui pourrait permettre d'en déterminer la clé.

10 Pour que ce courant I_{out} ne reflète plus les opérations effectuées, l'invention propose de le modifier par un dispositif 20 ou 30, disposé dans la puce 10 et connecté, par exemple, sur la borne d'entrée 16₁.

15 L'invention propose de modifier le courant de deux manières différentes. Une première en faisant en sorte que le dispositif 20 (figure 1) consomme du courant de manière aléatoire ou tout au moins irrégulière, consommation supplémentaire aléatoire qui s'ajoutant à
20 la consommation normale de courant I_{in} rend aléatoire la valeur I_{out} .

La deuxième manière consiste à moyenner la valeur de I_{in} , ce qui ne permet pas de détecter les variations de I_{in} dues aux opérations effectuées.

25 Dans le premier cas, le dispositif 20 peut être réalisé à l'aide de résistances 30, en fait des transistors, qui sont alimentées ou non selon les signaux aléatoires fournis par un générateur 28. Les courants circulant dans les résistances alimentées
30 augmentent, modifiant la valeur du courant total et masquant le courant dû aux calculs cryptographiques.

Dans le deuxième cas, la moyenne du courant I_{in} est obtenue par un intégrateur qui "lisse" les variations du courant I_{in} de manière à les effacer.

Selon l'invention, plusieurs dispositifs 20 ou 30, référencés 20₁ et 30₁ peuvent être connectés à différents endroits de la puce électronique, par exemple, sur le conducteur d'alimentation de l'unité centrale (référence 22). En outre, ces dispositifs 20, 20₁, 30 et 30₁ peuvent être connectés ou non selon que les opérations doivent être sécurisées ou non, les connexions s'effectueront sous la commande de signaux fournis par l'unité centrale 12 (traits discontinus).

10 L'invention propose une troisième manière de brouiller la valeur de I_{out} en effectuant des opérations à sécuriser, telles que des calculs cryptographiques, pendant certaines phases des opérations de programmation ou d'effacement de la mémoire 14, ces opérations étant sur la commande de l'unité centrale 12.

Cette troisième manière repose sur l'utilisation d'une mémoire 14 de type EEPROM qui a la capacité d'auto-écriture.

20 Dans un mode habituel de fonctionnement, le microprocesseur met en marche un circuit de programmation 24 de la mémoire 14 selon les étapes suivantes :

- 1 - mise en marche de la pompe de charge,
- 25 2 - présentation sur le bus de données de la dernière à écrire,
- 3 - présentation sur le bus d'adresse de l'adresse écriture,
- 4 - mise en marche de la programmation,
- 30 5 - attente d'un délai de programmation,
- 6 - arrêt de la programmation,
- 7 - arrêt de la pompe de charge.

La programmation d'une cellule EEPROM nécessitant d'injecter des charges électriques dans la cellule

programmée, les étapes 4, 5 et 6 s'accompagnent d'une sur-consommation de courant d'apparence chaotique qui dépend essentiellement de la valeur de V_{CC} , de l'adresse, de la valeur programmée et de la température du composant.

Afin de masquer l'empreinte de consommation de courant d'un calcul cryptographique par exemple, l'invention propose d'utiliser la consommation chaotique des étapes 4, 5 et 6 en réalisant le calcul cryptographique pendant l'étape 5 d'une durée de quelques millisecondes.

Pour ce faire, le calcul cryptographique s'effectue selon les étapes suivantes :

- 1 - mise en marche de la pompe de charge,
- 2 - présentation sur le bus de données d'une donnée aléatoire,
- 3 - présentation sur le bus d'adresse d'une adresse écriture,
- 4 - mise en marche de la programmation,
- 5 - effectuer le calcul cryptographique,
- 6 - arrêt de la programmation,
- 7 - arrêt de la pompe à charge.

Par ces étapes, l'empreinte de la consommation de courant due au calcul cryptographique de l'étape 5 est masquée par l'écriture de la donnée aléatoire dans une partie déterminée 26 de la mémoire EEPROM réservée à cette fonction.

Au lieu d'un calcul cryptographique, l'étape 5 peut consister en toute opération à sécuriser vis-à-vis de l'extérieur.

Par ailleurs, au lieu de faire ces opérations à sécuriser lors d'une écriture dans la mémoire 14, elles peuvent être faites lors d'un effacement de la mémoire 14.

REVENDEICATIONS

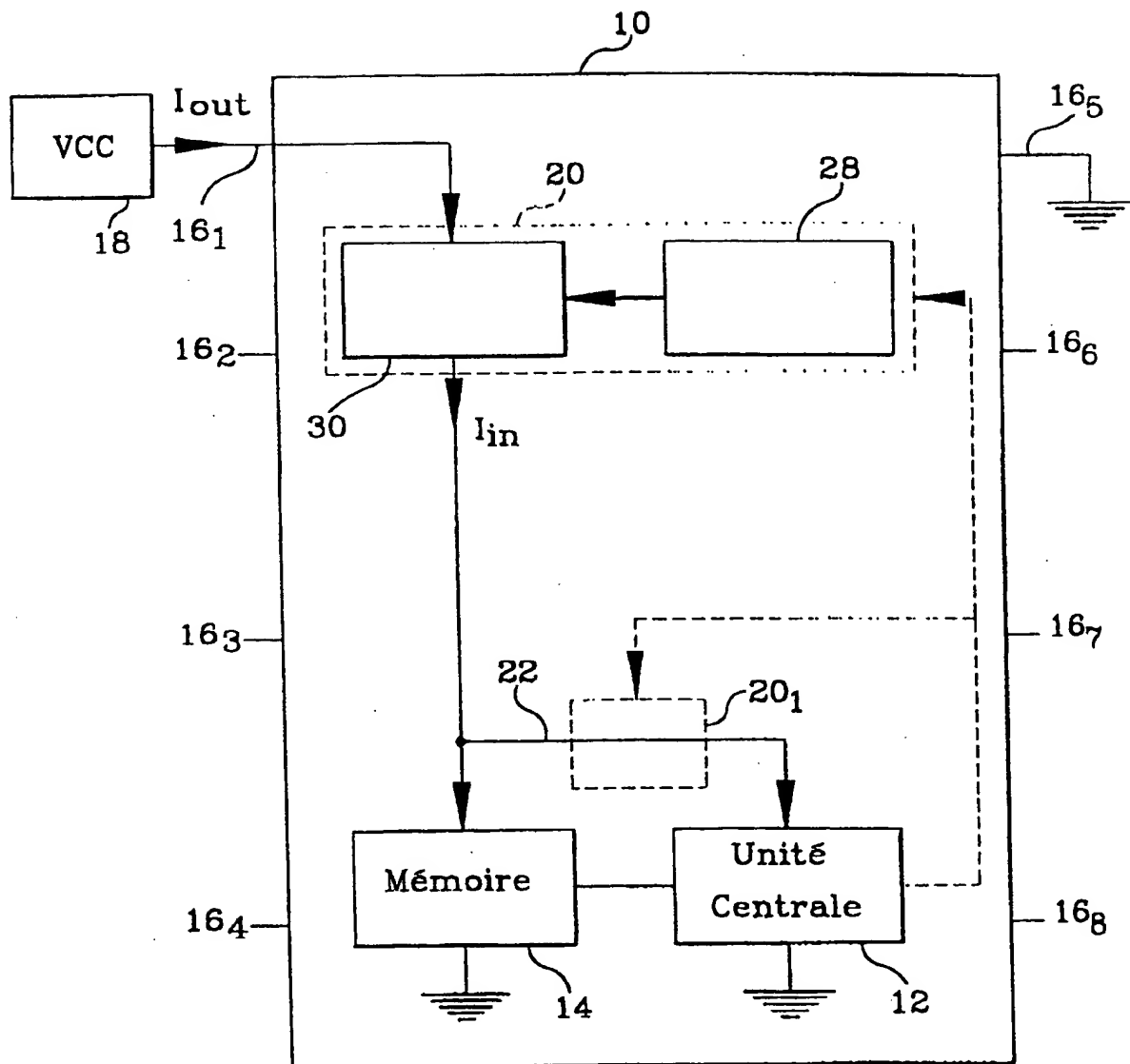
- 1 - Dispositif pour masquer les opérations effectuées par un composant destiné à être intégré à une carte à puce, caractérisé en ce qu'il comprend au moins un moyen (20, 30, 28, 26) pour modifier la consommation de courant dudit composant lors de la réalisation desdites opérations.
- 2 - Dispositif selon la revendication 1, caractérisé en ce que le moyen pour modifier la consommation de courant comprend au moins un circuit intégrateur (30) du courant du composant de manière à moyenner les variations de ce courant au cours du temps.
- 3 - Dispositif selon la revendication 1, caractérisé en ce que le moyen pour modifier la consommation de courant comprend au moins un générateur (28) de signaux aléatoires et une batterie de résistances (20) dont l'alimentation de chacune des résistances est commandée par les signaux aléatoires.
- 4 - Dispositif selon la revendication 1, caractérisé en qu'il comprend une pluralité de moyens (20, 20₁, 30, 30₁) pour modifier la consommation de courant.
- 5 - Dispositif selon la revendication 1, caractérisé en ce que le moyen pour modifier la consommation de courant du composant dans le cas d'une mémoire (14) du type EEPROM, consiste à effectuer simultanément:
 - une opération d'écriture ou d'effacement de la mémoire (14) dite de masquage, et
 - une opération du microprocesseur.
- 6 - Dispositif selon la revendication 5, caractérisé en ce que, pour mettre en oeuvre une opération d'écriture de masquage, la mémoire (14) comprend une partie (26) dédiée à l'enregistrement d'une donnée aléatoire.
- 7 - Dispositif selon l'une des revendications 1 à 5, caractérisé en ce que la mise en route de chacun des moyens de modification de la consommation de courant est commandée par le microprocesseur (12) de manière à être mis en route pour les seules opérations à sécuriser.
- 8 - Dispositif selon la revendication 5, caractérisé en ce que le microprocesseur (12) réalise au moins le calcul cryptographique selon les étapes suivantes:
 - mise en marche de la pompe de charge,
 - présentation sur le bus de données d'une donnée aléatoire,
 - présentation sur le bus d'adresse d'une adresse écriture,
 - mise en marche de la programmation,
 - effectuer le calcul cryptographique,
 - arrêt de la programmation,
 - arrêt de la pompe de charge,de manière à masquer l'empreinte de la consommation de courant occasionnée par ledit calcul cryptographique.

8

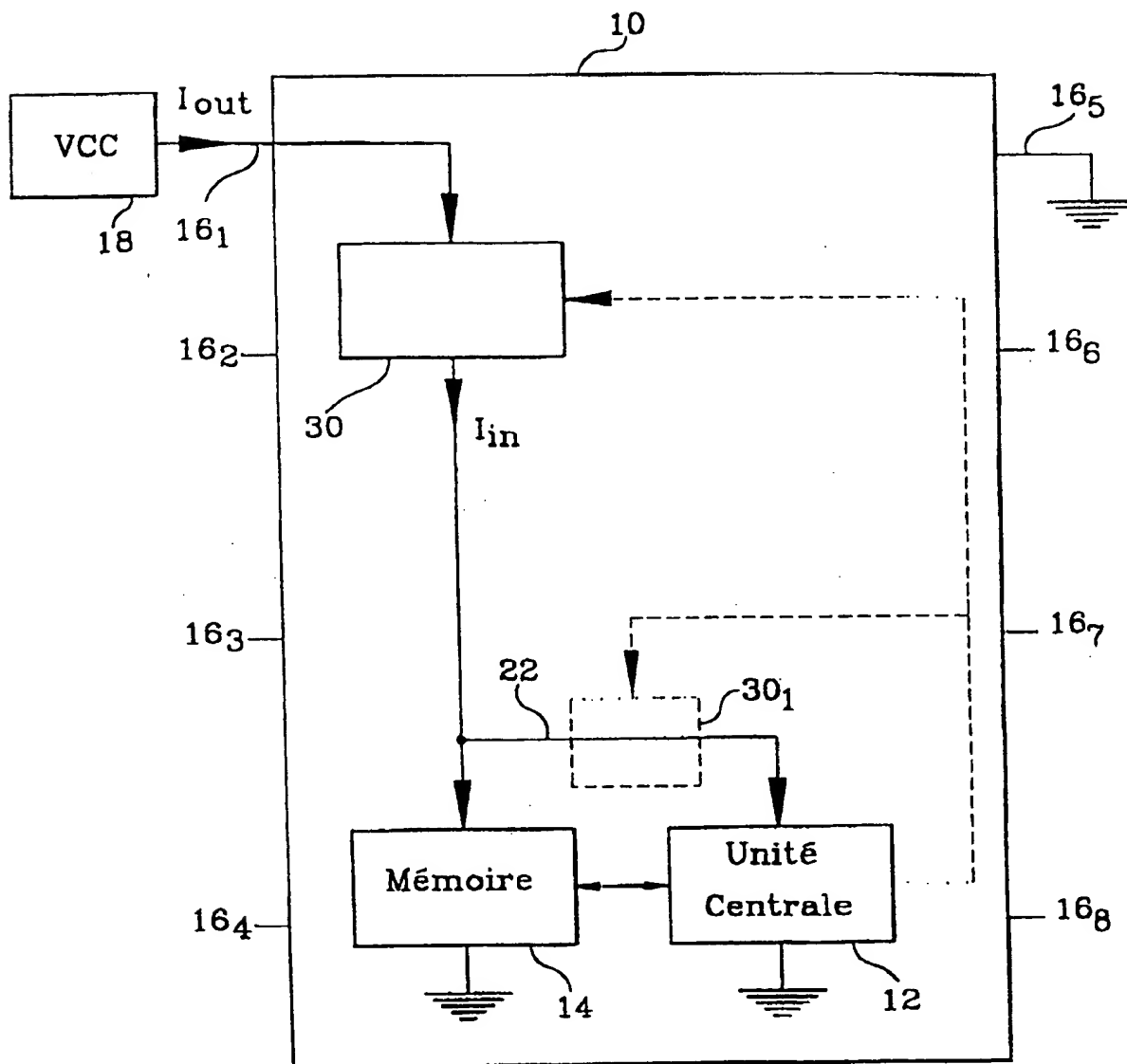
9 - Procédé pour masquer les opérations effectuées par un composant, caractérisé en ce qu'il comporte les étapes suivantes:

- mise en marche de la pompe de charge,
- présentation sur le bus de données d'une donnée aléatoire,
- présentation sur le bus d'adresse d'une adresse écriture,
- mise en marche de la programmation,
- effectuer le calcul cryptographique,
- arrêt de la programmation,
- arrêt de la pompe de charge.

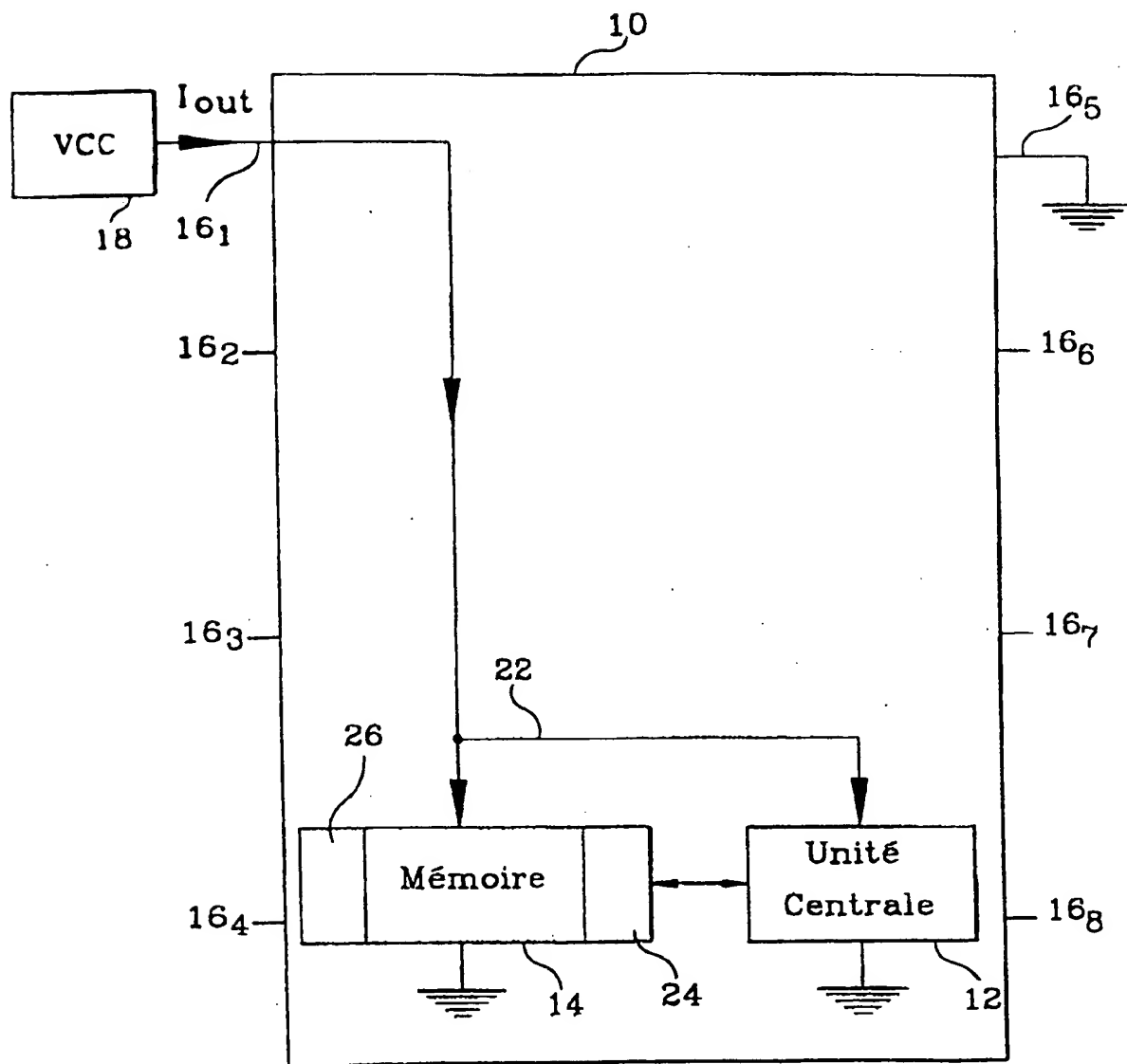
1/3

**FIG.1**

2/3

**FIG.2**

3/3

**FIG.3**

INTERNATIONAL SEARCH REPORT

International Application No

PCT/FR 99/00583

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06K19/073

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 6 G07F G06K G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 4 295 041 A (UGON MICHEL) 13 October 1981 see abstract; claim 1; figures 1,2 see column 1, line 61 - column 2, line 21 ---	1,5,7
X	US 4 932 053 A (FRUHAUF SERGE ET AL) 5 June 1990	1,3,4,7
Y	see abstract; figure 4 see column 2, line 29-59 see column 3, line 26 - column 4, line 21 ---	6
X	US 4 813 024 A (LISIMAQUE GILLES ET AL) 14 March 1989	1,5,7
Y	see column 2, line 8-31 see column 3, line 63 - column 4, line 13 see column 6, line 18-22 ---	6,8,9
	-/--	

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search

15 June 1999

Date of mailing of the international search report

21/06/1999

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Cardigos dos Reis, F

INTERNATIONAL SEARCH REPORT

International Application No

PCT/FR 99/00583

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	<p>WO 96 06504 A (CHANEY JOHN WILLIAM ; THOMSON CONSUMER ELECTRONICS (US)) 29 February 1996 see page 1, line 5-20 see page 2, line 3-10 see page 13, line 8-20 see page 22, line 9-18 -----</p>	8,9

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/FR 99/00583

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 4295041 A	13-10-1981	FR 2401459 A	23-03-1979
		FR 2460506 A	23-01-1981
		CH 631561 A	13-08-1982
		DE 2837201 A	01-03-1979
		DE 2858818 C	29-08-1996
		DE 2858819 C	09-03-1995
		DE 2858829 C	28-11-1996
		GB 2004394 A, B	28-03-1979
		JP 54046447 A	12-04-1979
		JP 62056556 B	26-11-1987
		JP 2506061 B	12-06-1996
		JP 7093501 A	07-04-1995
		JP 1826230 C	28-02-1994
		JP 2210590 A	21-08-1990
		JP 3050314 B	01-08-1991
		JP 1556417 C	23-04-1990
		JP 62070993 A	01-04-1987
		JP 63025393 B	25-05-1988
		JP 2097860 C	02-10-1996
		JP 5217034 A	27-08-1993
		JP 8007780 B	29-01-1996
		US 4211919 A	08-07-1980
		DE 3025044 A	27-05-1981
		JP 56038651 A	13-04-1981
		JP 2547379 B	23-10-1996
		JP 8110937 A	30-04-1996
		JP 1152589 A	15-06-1989
		JP 2043222 B	27-09-1990
		JP 2547368 B	23-10-1996
		JP 5274499 A	22-10-1993
US 4932053 A	05-06-1990	FR 2638869 A	11-05-1990
		EP 0368727 A	16-05-1990
		JP 2199561 A	07-08-1990
		JP 2813663 B	22-10-1998
US 4813024 A	14-03-1989	FR 2600183 A	18-12-1987
		DE 3777701 A	30-04-1992
		EP 0251853 A	07-01-1988
		JP 63080351 A	11-04-1988
WO 9606504 A	29-02-1996	AU 3238595 A	22-03-1996
		AU 701593 B	04-02-1999
		AU 3239495 A	14-03-1996
		BR 9508621 A	30-09-1997
		BR 9508622 A	19-05-1998
		CA 2196406 A	07-03-1996
		CA 2196407 A	29-02-1996
		CN 1158202 A	27-08-1997
		CN 1158203 A	27-08-1997
		EP 0878088 A	18-11-1998
		EP 0782807 A	09-07-1997
		FI 970677 A	18-02-1997
		JP 10506507 T	23-06-1998
		JP 10505720 T	02-06-1998
		PL 318647 A	07-07-1997
		WO 9607267 A	07-03-1996

RAPPORT DE RECHERCHE INTERNATIONALE

Den .de Internationale No

PCT/FR 99/00583

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 6 G06K19/073

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)

CIB 6 G07F G06K G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	US 4 295 041 A (UGON MICHEL) 13 octobre 1981 voir abrégé; revendication 1; figures 1,2 voir colonne 1, ligne 61 - colonne 2, ligne 21 ---	1,5,7
X	US 4 932 053 A (FRUHAUF SERGE ET AL) 5 juin 1990 voir abrégé; figure 4 voir colonne 2, ligne 29-59 voir colonne 3, ligne 26 - colonne 4, ligne 21 ---	1,3,4,7
Y	---	6
	--- -/--	

☒ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"Z" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

15 juin 1999

Date d'expédition du présent rapport de recherche internationale

21/06/1999

Nom et adresse postale de l'administration chargée de la recherche internationale
Office Européen des Brevets, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

Cardigos dos Reis, F

RAPPORT DE RECHERCHE INTERNATIONALE

Der. . . Je Internationale No

PCT/FR 99/00583

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Identification des documents cités, avec le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	US 4 813 024 A (LISIMAQUE GILLES ET AL) 14 mars 1989	1,5,7
Y	voir colonne 2, ligne 8-31 voir colonne 3, ligne 63 - colonne 4, ligne 13 voir colonne 6, ligne 18-22 ---	6,8,9
Y	WO 96 06504 A (CHANEY JOHN WILLIAM ;THOMSON CONSUMER ELECTRONICS (US)) 29 février 1996 voir page 1, ligne 5-20 voir page 2, ligne 3-10 voir page 13, ligne 8-20 voir page 22, ligne 9-18 -----	8,9

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Den. de internationale No

PCT/FR 99/00583

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 4295041	A	13-10-1981	FR 2401459 A	23-03-1979
			FR 2460506 A	23-01-1981
			CH 631561 A	13-08-1982
			DE 2837201 A	01-03-1979
			DE 2858818 C	29-08-1996
			DE 2858819 C	09-03-1995
			DE 2858829 C	28-11-1996
			GB 2004394 A, B	28-03-1979
			JP 54046447 A	12-04-1979
			JP 62056556 B	26-11-1987
			JP 2506061 B	12-06-1996
			JP 7093501 A	07-04-1995
			JP 1826230 C	28-02-1994
			JP 2210590 A	21-08-1990
			JP 3050314 B	01-08-1991
			JP 1556417 C	23-04-1990
			JP 62070993 A	01-04-1987
			JP 63025393 B	25-05-1988
			JP 2097860 C	02-10-1996
			JP 5217034 A	27-08-1993
			JP 8007780 B	29-01-1996
			US 4211919 A	08-07-1980
			DE 3025044 A	27-05-1981
			JP 56038651 A	13-04-1981
			JP 2547379 B	23-10-1996
			JP 8110937 A	30-04-1996
			JP 1152589 A	15-06-1989
			JP 2043222 B	27-09-1990
			JP 2547368 B	23-10-1996
			JP 5274499 A	22-10-1993
US 4932053	A	05-06-1990	FR 2638869 A	11-05-1990
			EP 0368727 A	16-05-1990
			JP 2199561 A	07-08-1990
			JP 2813663 B	22-10-1998
US 4813024	A	14-03-1989	FR 2600183 A	18-12-1987
			DE 3777701 A	30-04-1992
			EP 0251853 A	07-01-1988
			JP 63080351 A	11-04-1988
WO 9606504	A	29-02-1996	AU 3238595 A	22-03-1996
			AU 701593 B	04-02-1999
			AU 3239495 A	14-03-1996
			BR 9508621 A	30-09-1997
			BR 9508622 A	19-05-1998
			CA 2196406 A	07-03-1996
			CA 2196407 A	29-02-1996
			CN 1158202 A	27-08-1997
			CN 1158203 A	27-08-1997
			EP 0878088 A	18-11-1998
			EP 0782807 A	09-07-1997
			FI 970677 A	18-02-1997
			JP 10506507 T	23-06-1998
			JP 10505720 T	02-06-1998
			PL 318647 A	07-07-1997
			WO 9607267 A	07-03-1996

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.